ARTIGO DOI 10. 52781/cmm.145

A evolução e o futuro da Ciberguerra: um estudo aprofundado de Portugal

The evolution and Future of Cyberwar: an in-depth study of Portugal

Resumo: Este artigo analisa a guerra do futuro a partir da lente de análise da cibernética. O intuito é responder ao questionamento geral: como Portugal tem se organizado para travar a guerra do futuro? E, de forma mais específica: qual o papel da cibernética na preparação desse país? Adota-se, para tanto, a exploração e a análise global de documentos estratégicos do governo e das Forças Armadas portuguesas, os quais nos permitem entender em maior profundidade as dinâmicas do caso. O estudo revela a priorização e a atenção recém-conquistadas pelo domínio cibernético no país, com ações expressivas tais como a criação do Comando de Operações de Ciberdefesa.

Palavras-chave: Estratégia; Planejamento; Cibernética; Estudo de Caso; Portugal.

Abstract: This article understands the war of the future from the lens of cybernetics analysis. The aim is to answer the general question: how has Portugal organized itself to fight the war of the future? And, more specifically: what is the role of cybernetics in preparing this country? For this purpose, the exploration and global analysis of strategic documents from the government and the Portuguese Armed Forces is adopted, which allow us to understand in greater depth the dynamics of the case. The study reveals the prioritization and attention recently conquered by the cyber domain in the country, with significant actions such as the creation of the Cyberdefense Operations Command.

Keywords: Strategy; Planning; Cybernetics; Case Study; Portugal.

Natália Diniz Schwether
Universidade Federal de Santa Catarina
Florianópolis, SC, Brasil.
E-mail: n.schwether@unesp.br

Recebido: 7 jun. 2023
Aprovado: 27 set. 2024

COLEÇÃO MEIRA MATTOS
ISSN on-line 2316-4891 / ISSN print 2316-4833
http://ebrevistas.eb.mil.br/index.php/RMM/index

* O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001

1 INTRODUÇÃO

Na última década observamos a progressão na relevância do ciberespaço para o planejamento estratégico dos Estados e de suas respectivas Forças Armadas. No âmbito da Organização do Tratado do Atlântico Norte (OTAN), os Chefes de Estado e de Governo dos Estados-Membros anunciaram, em 2014, a ciberdefesa como um dos objetivos de defesa coletiva do grupo e, frente a isso, a necessidade de aprimoramento das capacidades nessa área (OTAN, 2014).

Alguns anos depois, em 2016, os Aliados reconheceram, formalmente, o ciberespaço como o quarto domínio das operações militares. E, mais recentemente, em 2022, o Conceito Estratégico da OTAN reafirmou que a utilização segura e o acesso sem restrições ao ciberespaço são fundamentais para uma efetiva dissuasão e defesa coletivas (OTAN, 2022).

No marco da União Europeia (UE), a ciberdefesa é, igualmente, uma área prioritária. Em 2020, a Estratégia de Cibersegurança da União Europeia afirmou o ciberespaço como um domínio da atividade militar. E, em 2022, a Bússola Estratégica firmou o compromisso de desenvolver uma política para o setor.

Portugal, Estado da Europa Meridional, membro da Comunidade Econômica Europeia desde 1986 e membro fundador da Aliança Atlântica, tem, também, em seu plano interno se dedicado a desenvolver um conjunto de iniciativas para garantir a utilização do ciberespaço de forma livre e segura (Pinho, 2020).

Entre elas destacam-se: o Conceito Estratégico de Defesa Nacional (2013), o qual apontou a cibercriminalidade como um dos principais riscos à segurança nacional, a definição de uma Orientação Política para a Ciberdefesa (2013), a criação do Centro de Ciberdefesa (CCD) das Forças Armadas (2014) e do Centro de Cibersegurança (CNCS) (2014), a Estratégia Nacional de Cibersegurança (2015 e 2019) e a Estratégia Nacional de Ciberdefesa (2022).

Nesse contexto, o Ministério da Defesa considerou a ciberdefesa como um dos projetos prioritários de sua pasta, bem como afirmou ser imperativo a qualificação dos recursos humanos afetos à área (Despacho nº10309/2022).

Diante disso, este artigo visa responder ao questionamento geral: como Portugal tem se organizado para travar a guerra do futuro? E, de forma mais específica: qual o papel da cibernética na preparação desse país? Haja vista a constante evolução da guerra, a qual desenvolve-se de maneira imprevisível, paralelamente, a expansão do campo de batalha, abrangendo uma ampla variedade de domínios e meios (cibernético, espacial, cognitivo e informacional) a serem, possivelmente, empregados pelos adversários no ambiente operacional futuro (Schwether, 2021).

Para isso, a principal estratégia de pesquisa será a exploratória, a qual ao realizar uma descrição dos principais documentos estratégicos portugueses produzidos na última década, permite-nos entender as etapas do planejamento em defesa e, em especial, como evoluiu e se organizou o setor cibernético.

A descrição é necessária quando se pretende responder perguntas: quando, quem, qual. A qualidade inferencial de uma descrição está diretamente relacionada com a qualidade das fontes de dados, dos instrumentos de medição ou dos procedimentos de codificação (Gerring, 2012).

Isto posto, essa introdução é seguida por três seções. A primeira delas aborda o que chamamos aqui de grande estratégia, ou seja, um plano com visão holística e multidimensional das prioridades de

ação de um Estado (Reis, 2019). Na segunda seção, o enfoque recai sobre o sistema de planejamento estratégico das Forças Armadas portuguesas, compilando os principais documentos que orientam a edificação das capacidades futuras. Na terceira seção, reduzimos o escopo da análise à capacidade cibernética e sua evolução a nível estratégico e organizacional. Por fim, a conclusão encerra ponderando os importantes avanços conquistados e os entraves ainda a serem enfrentados.

2 GRANDE ESTRATÉGIA

O vínculo estratégico transatlântico entre Estados Unidos, Canadá e Europa foi institucionalizado pelo Tratado do Atlântico Norte, em 1949. Essa relação é, desde então, fundamental para a definição das estratégias e políticas de defesa e segurança da Europa, bem como um instrumento essencial para a afirmação da política externa portuguesa.

Um dos documentos fundamentais formulados pela OTAN, o qual apresenta a visão estratégica para o futuro é o Conceito Estratégico (CE). Desde 1991, este documento define publicamente as prioridades estratégicas da Aliança e fornece orientações importantes para as instituições militares dos 32 Estados-membros. Prontamente, a importância de que os interesses nacionais portugueses estejam refletidos nos grandes princípios comuns acordados e o planejamento nacional observe essa publicação (Reis, 2022; Serronha, 2010).

O CE aprovado no final de 2010, em Lisboa, centrou-se em três questões: defesa coletiva, gestão de crises e segurança cooperativa. Um dos pontos mais relevantes desse documento trata do alargamento do raio de ação da Organização, isto é, estando um membro em risco, a Aliança pode agir externamente às próprias fronteiras. Expressou, ainda, um propósito de envolvimento ativo na segurança internacional ao propor parcerias com outros países e organizações (Fernandes, 2013).

Entretanto, em termos de política externa portuguesa, deixou de incorporar várias questões ambicionadas pela diplomacia do país, especialmente, no que se refere ao alargamento das parcerias rumo ao Atlântico Sul (Fernandes, 2013). A vocação marítima de Portugal é central para a afirmação do país no contexto internacional e o Atlântico é uma área de interesse estratégico.

Dez anos após a aprovação do último CE e em um cenário de crescente digitalização da sociedade e complexidade do contexto global de segurança e defesa, foi iniciado mais um processo formal de revisão do documento.

O CE de Madrid, aprovado em 2022, ao mesmo tempo que reafirmou princípios centrais da Organização[1], apresentou, também, uma nova lista de potenciais adversários, com a inclusão de China e Rússia. Além de ressaltar o surgimento das novas tecnologias e o interesse crescente nos domínios espacial e cibernético (Daehnhardt; Gaspar, 2020; Gaspar, 2022; Garcia, 2022; Daehnhardt, 2022).

O CE é um dos principais insumos para a formulação, em Portugal, do Conceito Estratégico de Defesa Nacional (CEDN). O CEDN é o principal instrumento de apresentação da estratégia nacional para a defesa e a segurança e uma ferramenta de coordenação dos esforços das diversas agências estatais na mitigação das preocupações nacionais[2] (Portugal, 2013a).

1 São princípios centrais a defesa coletiva e a dissuasão.

2 São elas: terrorismo, proliferação de armas de destruição massiva, criminalidade transnacional organizada, cibercriminalidade e pirataria

O documento, aprovado em 2013, recomenda às Forças Armadas uma atuação conjunta, que perpasse todas as esferas da instituição, desde os conceitos, doutrinas, procedimentos até a cultura institucional e organizacional. Afora propor uma reorganização e simplificação das estruturas, com vistas a uma maior eficiência, agilidade, modularidade e flexibilidade. A nível de planejamento estratégico, o CEDN determinou que os investimentos passassem a ser orientados conforme as capacidades necessárias ao cumprimento das missões prioritárias (Portugal, 2013a).

Em específico sobre o meio cibernético foram traçados alguns objetivos, entre eles, a definição de uma Estratégia Nacional de Cibersegurança, a criação de órgãos técnicos, a sensibilização de usuários e o aprimoramento da capacidade de ciberdefesa nacional. Para isso, uma melhor comunicação estratégica das Forças Armadas e a promoção da pesquisa e inovação seriam prementes (Portugal, 2013a).

Afinal, embora o componente tecnológico seja, muitas vezes, uma condição inicial importante para as inovações, uma verdadeira revolução militar depende da confluência entre armas, operações, organização e visão da guerra futura (Adamsky, 2010). Tão importante quanto é o papel do Estado, enquanto agente propulsor, capaz de investir em pesquisas, definir áreas prioritárias e formular estratégias de longo prazo (Storti; Ferreira, 2022).

Em outras palavras, à medida que o futuro da guerra coloca mais exigências e movimenta os limitados recursos dos Estados em direções opostas, são eles os responsáveis por realizar as grandes escolhas estratégicas (Cohen *et al*., 2020).

Na esteira desse pensamento, seja pelos reflexos da crise pandêmica ou pelo fim da paz no continente europeu, em 2022, tornou-se imperativo iniciar um processo de revisão do CEDN, fomentado por um conjunto de iniciativas para promoção do debate público sobre os temas de interesse e por personalidades de reconhecido mérito, que se reuniram para refletir as questões (Conselho, 2023).

Em 2023, foi apresentado o Relatório de Revisão do Conceito Estratégico de Defesa Nacional. A proposta, aprovada em maio, constitui parte integrante do processo de revisão do CEDN e integrará a versão final a ser aprovada pela resolução do Conselho de Ministros, Primeiro-Ministro e Ministro da Defesa Nacional.

No documento, a disputa pelo domínio do ciberespaço e a ampliação das capacidades cibernéticas de atores estatais e não estatais foram apontadas como desafios à estabilidade estratégica e à segurança. Assim como a competição no ciberespaço e a sofisticação dos ataques e dos danos que podem infligir, especialmente às infraestruturas críticas, foi considerada uma das maiores ameaças, difícil de se antecipar e suscetível de atingir funções sociais básicas e o bem-estar dos cidadãos (Conselho, 2023).

Foi, ainda, categórico ao afirmar ser primordial melhorar as capacidades de defesa e de resiliência do país, ademais de reforçar a cooperação no domínio da defesa, aumentar a capacidade da indústria militar e reforçar as capacidades das Forças Armadas, assegurando as estruturas e os mecanismos necessários a uma ação integrada nos diferentes domínios operacionais (Conselho, 2023).

Em específico, recomendou desenvolver a capacidade nacional nas dimensões do espaço e do ciberespaço e programar a aquisição de novos meios, equipamentos e sistemas para edificar, em médio e longo prazo, o espectro completo das capacidades militares. Paralelamente à valorização

e qualificação da dimensão humana da Força, aprofundando o processo de profissionalização do sistema militar (Conselho, 2023).

Os analistas sugeriram, por fim, horizontes temporais mais curtos de revisão, a implementação de mecanismos de acompanhamento das ações, tal e qual uma alteração no nome do documento, de Conceito Estratégico de Defesa Nacional para Estratégia de Segurança e Defesa. Futuramente, o documento poderia ser base para uma Estratégia de Segurança Nacional (Conselho, 2023)[3].

3 PLANEJAMENTO ESTRATÉGICO EM DEFESA

Portugal possui um sistema de planejamento estratégico que, nos seus aspectos essenciais, se mantém inalterado há cerca de quatro décadas. Instituído na década de 1980, foi pensado para ser desenvolvido de forma sequencial e hierárquica, em várias fases, começando pelo CEDN (abordado na seção anterior), a que se segue o Conceito Estratégico Militar (CEM), a definição das Missões das Forças Armadas (MIFA), do Sistema de Forças Nacional (SF) e do Dispositivo de Forças (Rodrigues, 2020).

Figura 1. Planejamento Estratégico de Defesa

Fonte: Elaborado pela autora, 2023.

O CEM, entre outros, identifica os objetivos estratégicos militares, as modalidades de ação militar para atingir tais objetivos e aporta recomendações em termos de meios. É de competência do Ministério da Defesa Nacional, por proposta do Conselho de Chefes de Estado Maior (Rodrigues, 2020).

O documento, aprovado em 2014, é, até a sua revisão, o principal instrumento nacional a orientar a edificação das capacidades futuras, conforme os cenários de emprego, objetivos militares

3 A proposta está em linha com a percepção de Rodrigues (2020), para o autor o que se designa em Portugal por CEDN é, de fato, uma estratégia e não um conceito e, sendo assim, deve garantir uma harmonia entre os objetivos e meios. Um conceito operacional constitui essencialmente a formulação de uma ideia relativamente à forma como algo poderá ser feito ou concretizado e que poderá, por isso, conduzir a um determinado procedimento ou capacidade. Os conceitos constituem normalmente uma visão da forma como as Forças Armadas pretendem vir a operar no médio e longo prazo, baseando-se em alterações observadas no cenário ou nos domínios estratégicos. Os conceitos contêm normalmente elementos resultantes da combinação de uma avaliação informada e de um pensamento inovador (Nunes, 2016).

e níveis de ambição nele definidos. Em específico sobre os casos de ciberataques, instrui que as Forças Armadas serão chamadas a intervir para:

> [...] garantir a salvaguarda da sua informação e a proteção das suas infraestruturas de comunicações e dos sistemas de informação, apoiarão na proteção e defesa das infraestruturas críticas nacionais, bem como colaborarão com outras instituições do Estado no âmbito da cibersegurança, contribuindo para a proteção das populações e promoção do seu bem-estar (Portugal, 2023).

Outrossim, aponta para a preocupação em obter capacidades diversificadas, interoperáveis e integráveis, bem como a pretensão de organizar as Forças Armadas com ênfase no emprego modular, flexível, conjunto e combinado. Embora, seja digno de nota que a ausência de um horizonte temporal definido torne as indicações pouco precisas para um planejamento de longo prazo das Forças Armadas (Abreu, 2018; Pires, 2018).

As MIFAs têm como finalidade identificar as missões de nível estratégico-militar designadas às Forças Armadas e correspondentes às tarefas militares concretas. A execução das missões respeita às prioridades e orientações contidas no CEDN e no CEM.

Nas MIFAs, apresentadas em 2014, as missões concentram-se em seis áreas: (a) segurança e defesa do território nacional e dos cidadãos; (b) defesa coletiva; (c) exercício da soberania, jurisdição e responsabilidades nacionais; (d) segurança cooperativa; (e) apoio ao desenvolvimento e bem-estar; e (f) cooperação e assistência militar.

Para a defesa do território nacional se prevê a possibilidade de:

> [...] aplicar medidas de cáracter defensivo e se necessário ofensivo contra ataques cibernéticos, a fim de garantir a salvaguarda da informação e a proteção das infraestruturas de Comunicações e dos Sistemas de Informação das Forças Armadas, bem como, o apoio na proteção e defesa das infraestruturas críticas nacionais e do governo eletrônico do Estado (Portugal, 2014, p. 3, grifo nosso).

O SF identifica um conjunto de capacidades que devem existir para o cumprimento das missões das Forças Armadas, indicando os tipos e quantitativos de forças e meios, a partir de orientações específicas, cenários de emprego e da complementaridade operacional.

O documento, entretanto, priva-se de ser uma referência para o desenvolvimento de programas e para o reequipamento militar por se restringir a ser uma listagem das unidades, infraestruturas, órgãos, etc., e não apresentar uma visão de futuro ou antecipar necessidades de modernização (Rodrigues, 2003).

Por sua vez, o Dispositivo de Forças estabelece a relação entre os comandos operacionais, Forças, unidades e meios com as infraestruturas que lhes dão suporte, materializando a forma como se organizam e respondem a várias capacidades elencadas no SF para o cumprimento das MIFA.

Finalmente, é a Lei de Programação Militar (LPM) o instrumento financeiro de materialização da estratégia militar capaz de dotar as Forças Armadas com as capacidades

militares necessárias para o cumprimento das suas missões no que tange ao material (manutenção, substituição ou inovação) (Abreu, 2018).

Entre os projetos incluídos na LPM está a ciberdefesa, particularmente, a proteção e a segurança das redes informáticas de infraestruturas críticas e sistemas de Comando e Controle e a dotação de capacidade ofensiva às Forças Armadas para neutralizar potenciais ameaças. Ao comparar as LPM de 2015 e 2019, observa-se um importante incremento nos investimentos direcionados ao setor e à manutenção dos recursos para o período 2023-2034[4].

Não obstante, seja digno de nota que o orçamento destinado à ciberdefesa nunca tenha sido executado a mais de 50%[5], seja devido à pandemia, à escassez de recursos humanos especializados ou à demora na tramitação de processos (Marcelino, 2023).

Outrossim, o ciclo de planejamento estratégico 2014-2019 foi orientado pelo documento Reforma Defesa 2020, de abril de 2013, o qual considerou estabelecer Forças Armadas mais modernas, operacionais, sustentáveis e eficientes. As orientações foram divididas em dois pilares: (i) novo ciclo de planejamento estratégico e (ii) reorganização da macroestrutura. Em termos de estrutura, prezou-se pela natureza conjunta, modular e flexível. Entre as orientações específicas estava: o aumento da capacidade de ciberdefesa (Portugal, 2013b).

Mais recentemente, a Diretiva Ministerial de Planeamento de Defesa Militar, quadriênio 2019-2022, aprovada em 2020, seguiu reforçando a dimensão de comando conjunto das Forças e a relevância de integrar, com a máxima eficácia, o componente terrestre, naval e aéreo, assim como as capacidades de atuação no ciberespaço (Portugal, 2020).

Salientou, sobretudo, o empenho em pensar a defesa nacional, mais especificamente, a renovação da estrutura, da doutrina e dos meios, à luz dos novos desafios como, por exemplo, o espaço e o ciberespaço, a inteligência artificial e a desinformação. E fazê-lo, tendo em vista a frequência e a intensidade crescente dos ciberataques e o desafio de novos atores, novas tecnologias e novos domínios (Portugal, 2020).

4 AÇÕES NO CIBERESPAÇO

A primeira iniciativa, em nível estratégico, foi, ainda em 2013, com a promulgação da Orientação Política para a Ciberdefesa, diretiva que forneceria substrato para edificar a capacidade no setor.

O referido documento estabeleceu três grandes objetivos: (i) garantir a proteção, resiliência e a segurança das redes contra-ataques; (ii) liberdade de ação do país no ciberespaço – assegurar e, quando necessário, impedir ou dificultar o seu uso hostil contra o interesse nacional; e (iii) contribuir de forma colaborativa no contexto nacional (Portugal, 2013c).

Para a consecução desses objetivos foram definidas sete linhas de ação: (1) estabelecimento da estrutura de ciberdefesa nacional; (2) integração das operações no ciberespaço no âmbito das capacidades militares; (3) conduzir todo o espectro de operações militares no ciberespaço;

4 LPM 2015-2026 total de recursos para Ciberdefesa 14.000; LPM 2019-2030 total de recursos para a Ciberdefesa 45.490; LPM 2023-2034 total de recursos para a Ciberdefesa 43.469.

5 Em 2020 apenas 48,9%; em 2021 caiu para 27% e em 2022 ficou nos 30,7% (Marcelino, 2023).

(4) reforçar a capacidade de informações no ciberespaço; (5) desenvolver um sistema de alerta imediato e partilha de informação aos vários níveis e patamares de decisão; (6) promover uma cultura de gestão do risco por meio da incorporação de requisitos de gestão de risco nas aquisições a realizar e na cadeia de abastecimento; e, (7) centralizar a formação e o treino em ciberdefesa e adequar a gestão dos recursos humanos de modo a garantir a sua permanência nessas atividades (Portugal, 2013c).

O documento identificou, ainda, a necessidade de se estabelecer parcerias entre instituições estatais e privadas, nacionais e internacionais, como forma de promover o desenvolvimento tecnológico, a pesquisa e a inovação (Portugal, 2013c).

Em 2015, a ciberdefesa teve os seus contornos melhores definidos com a publicação da Estratégia Nacional de Segurança do Ciberespaço (ENSC). A Estratégia ambicionava aprofundar a segurança das redes e dos sistemas de informação e permitir uma utilização livre, segura e eficiente do ciberespaço (Portugal, 2015).

Para tanto, foram definidos seis eixos de intervenção, a saber: Eixo 1: Estrutura de segurança do ciberespaço; Eixo 2: Combate ao cibercrime; Eixo 3: Proteção do ciberespaço e das infraestruturas; Eixo 4: Educação, sensibilização e prevenção; Eixo 5: Investigação e desenvolvimento; Eixo 6: Cooperação. Do primeiro eixo é possível extrair funções atribuídas especificamente à defesa nacional, quais sejam:

> a) Concretizar a Orientação Política para a Ciberdefesa, aprovada pelo Despacho n.º 13692/2013, de 11 de outubro, publicado no Diário da República n.º 208, 2.ª série, de 28 de outubro, edificando a estrutura de ciberdefesa nacional;
>
> b) Estabelecer e consolidar uma estrutura de comando e controlo da ciberdefesa nacional [...];
>
> c) Implementar, desenvolver e consolidar a capacidade de ciberdefesa, com vista a assegurar a condução de operações militares no ciberespaço, assegurando a liberdade de ação do país no ciberespaço e, quando necessário e determinado, a exploração proativa do ciberespaço para impedir ou dificultar o seu uso hostil contra o interesse nacional;
>
> d) Constituir a ciberdefesa uma área onde é necessário promover sinergias e potenciar o emprego dual das suas capacidades, no âmbito das operações militares e da cibersegurança nacional, desenvolvendo e consolidando um sistema de partilha de informação aos vários níveis e patamares de decisão (Portugal, 2015, grifo nosso).

O documento, ao final, situou a importância de produzir uma revisão regular e periódica, em um prazo máximo de três anos, assim como de proceder uma verificação anual dos objetivos estratégicos e das linhas de ação, frente à evolução das circunstâncias (Portugal, 2015).

Desta feita, em 2019, foi aprovada a segunda Estratégia Nacional de Segurança do Ciberespaço de Portugal, assente em três objetivos estratégicos: maximizar a resiliência,

promover a inovação e gerar e garantir recursos, os quais foram traduzidos em seis eixos de intervenção, bastante similares aos da versão anterior (Portugal, 2019).

No que tange à ciberdefesa, buscar-se-á reforçar a resiliência das Forças Armadas, devendo ser utilizado todos os meios para responder a ciberataques, incluindo a capacidade ofensiva. Paralelamente, pretendia-se maximizar a segurança e a defesa das redes e sistemas de informação por meio da capacidade de ciberdefesa defensiva (Portugal, 2019).

Refere, ainda, a necessidade de aprofundar o emprego dual das capacidades de ciberdefesa, desenvolvendo e consolidando um sistema de compartilhamento de informação aos vários níveis e patamares de decisão. Além de participar nos exercícios de cibersegurança e ciberdefesa, tendo em vista a cooperação internacional e a afirmação de Portugal nesse domínio (Portugal, 2019).

Na esteira da ENSC e diante da constatação da premência de densificar conceitos em nível estratégico e de, devidamente, articular as estruturas dedicadas ao ciberespaço, foi publicada, em novembro de 2022, a Estratégia Nacional de Ciberdefesa (ENCD) (Nunes, 2018).

A ENCD reafirma o ciberespaço como um domínio das operações militares, defensivas e ofensivas, sendo as últimas de exclusividade das Forças Armadas, como forma de assegurar a defesa e os interesses nacionais, em resposta às ameaças originárias de Estados ou entidades não estatais e dependente de autorização política (Portugal, 2022a).

Nesse sentido, estabelece que o desenvolvimento da capacidade cibernética deve estar em conformidade com os demais documentos orientadores da defesa militar; isto é, o ciberespaço é um elemento integrante do processo de planejamento, que preza por uma lógica multidomínio e com flexibilidade operacional, devendo as Forças Armadas assegurar todas as capacidades de comando e controle relevantes a este novo domínio (Portugal, 2022a).

Foram definidos, ainda, quatro objetivos estratégicos: consolidar a capacidade de ciberdefesa; maximizar a resiliência e a coesão da ação nacional; promover a investigação, desenvolvimento e inovação; garantir recursos qualificados. E, seis eixos orientadores para o plano de ação: Eixo 1: utilizar o ciberespaço como um domínio de operações; Eixo 2: reforçar a capacidade de ciberdefesa nacional; Eixo 3: criar a escola de ciberdefesa; Eixo 4: intensificar a cooperação nacional e internacional; Eixo 5: promover a investigação, desenvolvimento e inovação no ciberespaço, incentivando o desenvolvimento de soluções de duplo uso; Eixo 6: assegurar as capacidades necessárias da ciberdefesa em contextos de estado de exceção (Portugal, 2022a).

No tocante ao reforço da capacidade, três linhas de ação são prioritárias: o incremento de pessoal qualificado, deter uma infraestrutura tecnologicamente avançada e garantir a independência tecnológica, promovendo, por exemplo, a indústria 4.0. Com especial atenção ao recrutamento, seleção, retenção e capacitação da componente humana (Portugal, 2022a, Serra, 2019).

Inclusive propôs a edificação de uma entidade formadora no âmbito das Forças Armadas e em colaboração com outras entidades nacionais e internacionais de referência. Julgou, igualmente, importante a participação ativa nos mecanismos de gestão de crises, em exercícios e organismos internacionais com atuação na segurança do ciberespaço (Portugal, 2022).

A nível organizacional, em 2014, foi criado o Centro de Ciberdefesa (CCD) das Forças Armadas. A concepção do CCD, à data, revela o alinhamento com o pensamento estratégico da instituição. O CCD integra a estrutura do Estado-Maior-General das Forças Armadas (EMGFA) e é constituído por militares dos três ramos, sua missão precípua é garantir a integridade, a

confidencialidade e a disponibilidade de informação e dos sistemas de informação da defesa nacional (Portugal, s.d).

Mais recentemente, a Lei Orgânica do Estado-Maior-General das Forças Armadas, de 2022, alterou a estrutura, até então destinada à ciberdefesa. Com a sua aprovação, o EMGFA teve sua missão ampliada, contemplando, para além do emprego das Forças Armadas em missões e tarefas operacionais, a estratégia de defesa militar, o ensino superior militar, a saúde militar, as informações e segurança militares, a ciberdefesa, os aspectos militares do programa espacial da defesa nacional e a inovação e transformação nas Forças Armadas (Portugal, 2022b).

As novas atribuições do EMGFA visam garantir o princípio fundamental da unidade de comando e coordenação, bem como dão continuidade ao processo de adaptação das Forças Armadas para que possam operar no multidomínio e enfrentar ameaças transnacionais e híbridas (Portugal, 2022b).

Ao domínio cibernético foram criadas duas estruturas: o Centro de Comunicações e Informação, Ciberespaço e Espaço (CCICE), na direta dependência do Chefe do Estado Maior General das Forças Armadas (CEMGFA) e o Comando de Operações de Ciberdefesa (COCiber) (Portugal, 2022b).

O CCICE tem como missão habilitar a capacidade de Comando e Controle conjunto das Forças Armadas, assegurar o exercício do comando de operações militares no e através do ciberespaço pelo CEMGFA e dirigir os aspectos militares do programa espacial de defesa nacional (Portugal, 2022b).

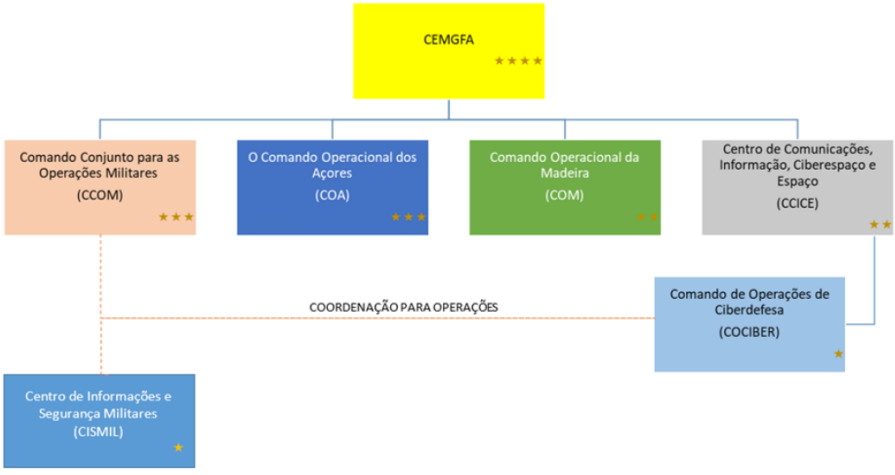
Compete ao CCICE planejar, coordenar e executar as medidas de segurança dos sistemas de informação e das comunicações e de resposta a incidentes para a proteção e resiliência da infraestrutura tecnológica conjunta, bem como propor e conduzir operações militares no e através do ciberespaço em apoio a objetivos militares, participar e organizar exercícios conjuntos e combinados de ciberdefesa, disponibilizar e coordenar a capacidade de ciberdefesa, atuar em articulação e estreita cooperação com as estruturas nacionais responsáveis pela segurança do ciberespaço. O órgão compreenderá em sua estrutura a Escola de Ciberdefesa (ECD) (Portugal, 2022b).

O COCiber é responsável pelo planejamento, direção, controle e execução de operações no e através do ciberespaço. A estrutura do COCiber pode ser reforçada por elementos ou unidades dos ramos das Forças, bem como para o desenvolvimento de operações e para o planejamento e condução de exercícios conjuntos ou combinados. Relaciona-se, também, com as estruturas internacionais ligadas à ciberdefesa e a ciberesegurança no âmbito da OTAN e da UE. Sua estrutura compreende a Força de Operações de Ciberdefesa (Portugal, 2022b).

Em termos de cibersegurança, cada Força é responsável pela resposta a incidentes dos seus CIS, sob coordenação do COCiber. Havendo um incidente que a Força não consiga resolver de forma autónoma, o COCiber assume o controle tático, ficando responsável pela resposta ao incidente (Pereira, R., 2022b).

O COCiber visa contribuir para uma melhor articulação operacional, potencializando a coordenação entre o EMGFA e os braços das Forças, além de prever uma relação direta com o Comando Conjunto para as Operações Militares (CCOM), o que irá aproximar o ciberespaço dos demais domínios da guerra (Pereira, B., 2022).

Figura 2. Organograma da Defesa



Fonte: Bruno Pereira (2022).

Destarte, com a reestruturação da capacidade cibernética, as componentes de ciberdefesa de cada Força ficaram sob a esfera do COCiber, viabilizando maior interoperabilidade e conferindo ao Comando um papel central na ciberdefesa nacional (Nunes, 2020).

Relativamente ao vetor material, o Plano de Desenvolvimento da Capacidade de Ciberdefesa (PDCCD) 2021-2021 afirma que deve ser garantida a evolução e a manutenção das soluções tecnológicas da infraestrutura digital da defesa nacional (Pereira, B., 2022).

A nível de pessoal, em 2023, foi criada a *Cyber Academia and Innovation Hub* (CAIH), a qual tem como missão o desenvolvimento de atividades de interesse público que visam promover a formação, treinamento e exercícios, bem como estimular a pesquisa, o desenvolvimento e a inovação no domínio do ciberespaço. De forma a fomentar o conhecimento e as competências necessárias a uma nova geração de profissionais na área da cibersegurança e da ciberdefesa (Portugal, 2023).

Para além disso, a Direção Geral dos Recursos Humanos (RH) da Defesa Nacional desenvolveu uma política de RH para a ciberdefesa, com a qual pretende atender as necessidades de recrutamento, formação e retenção de civis ou militares para atuar, principalmente, como: ciberdefensores, operadores, analistas forenses ou programadores de ciberdefesa (Pereira, B., 2022).

No âmbito do ensino superior militar, a formação em ciberdefesa desenvolveu-se, inicialmente, na Academia Militar com uma pós-graduação em ciberdefesa e ciberesegurança, a isso se seguiu a Escola Naval com um Mestrado em Segurança da Informação e Direito no Ciberespaço e o Instituto Universitário Militar, que também desenvolveu formação e treinamento na área (Pereira, B., 2022).

No ambiente internacional, as atividades de cooperação multilateral remontam a 2013, quando Portugal assumiu a liderança no projeto *Multinational Cyber Defense Education and Training* (MN CD E&T), da OTAN. O objetivo do projeto era criar uma plataforma de coordenação de ensino e treinamento em ciberdefesa e desenvolver novas iniciativas, contribuindo para o desenvolvimento das capacidades na área e a interoperabilidade no âmbito da OTAN.

Em 2017, Portugal aderiu ao *Cooperative Cyber Defence Center of Excellence* (CCDCOE), da OTAN, arquitetado para potencializar o treinamento, formação e capacitação no domínio da ciberdefesa. E, em 2019, foi instalada, no país, a principal sede da *Communications and Information Academy* (NCI Academy), a qual reúne todas as atividades associadas à educação e ao treinamento fornecidos pela Agência, especialmente àquelas relacionadas ao ciberespaço.

Portugal participa, ainda, de exercícios como o *Coalition Warrior Interoperability Exploration, Experimentation, Examination Exercise* (CWIX), um exercício anual projetado para aprimorar a interoperabilidade entre os membros da Aliança e as nações parceiras e o *Cyber Coalition*, um dos maiores exercícios de ciberdefesa do mundo.

5 CONCLUSÃO

Destarte, ao longo deste artigo foi possível depreender a crescente expressão que o setor cibernético conquistou na organização da defesa portuguesa. Embora, os documentos norteadores do planejamento estratégico do país remontem a 2014 e careçam de uma pronta atualização, verifica-se que já naquela altura eram consideradas ações, defensivas e ofensivas, nesse domínio, de forma a assegurar os interesses nacionais.

Mais do que isso, considerando a proposta, já aprovada, que orientará a confecção de um novo CEDN, na qual o ciberespaço ganhou mais destaque, à semelhança das LPMs de 2019 e 2023 em que o setor recebeu maior dotação orçamentária, lado a lado às iniciativas de produção de documentos estratégicos específicos e às reformas organizacionais, com destaque para a criação do COCiber, são importantes indicadores de que o domínio cibernético tem ganhado proeminência estratégica nas operações presentes e futuras.

Em um cenário em que as Forças Armadas devem estar preparadas para atuar de forma interoperável e em múltiplos domínios, o compartilhamento de treinamentos, exercícios e dados, bem como a capacitação e a retenção de pessoal qualificado, somado aos investimentos em tecnologias de ponta, são elementos indispensáveis ao planejamento estratégico em defesa. Nessa seara, a capacidade cibernética é instrumento crucial, em tempos de guerra e de paz, para a segurança e prosperidade dos países.

À vista disso, Portugal, sem dúvidas, deu passos cruciais nos últimos anos no levantamento de sua ciberdefesa, embora ainda deva superar entraves importantes, a exemplo da não execução do investimento previsto, em 2022, para capacitar o Centro de Ciberdefesa, o qual segue aquém das necessidades em termos qualitativos e quantitativos e do significativo atraso na criação da Escola de Ciberdefesa. Fatos que aumentam as expectativas para o, recém-iniciado, novo ciclo de planejamento estratégico da defesa.

REFERÊNCIAS

ABREU, M. das N. **O Planeamento de Longo Prazo e a Renovação de Sistemas de Armas para o Período 2020-2035**. Trabalho de Investigação Individual do CPOG 2017/2018. Pedrouços: Instituo Universitário Militar, 2018.

ADAMSKY, D. **The Culture of Military Innovation**: The impact of cultural factors on the revolution in military affairs in Russia, the US, and Israel. Stanford: Stanford University Press, 2010.

COHEN, R.; CHANDLER, N.; EFRON, S.; FREDERICK, B.; HAN, E.; KLEIN, K.; MORGAN, F.; RHOADES, A.; SHATZ, H.; SHOKH, Y. **The Future of Warfare in 2030**. Santa Monica: Rand Corporation, 2020.

CONSELHO DE REVISÃO DO CONCEITO ESTRATÉGICO DE DEFESA NACIONAL. **Ciclo de Revisão do Conceito Estratégico de Defesa Nacional 2022-2023**. Lisboa: Ministério da Defesa da Defesa Nacional, 2023. Disponível em: https://www.idn.gov.pt/pt/noticias/Paginas/Ciclo-de-Revis%C3%A3o-do-Conceito-Estrat%C3%A9gico-de-Defesa-Nacional.aspx. Acesso em: 23 out. 2024.

DAEHNHARDT, P.; GASPAR, C. Portugal e a Revisão do Conceito Estratégico da NATO. **Relações Internacionais**, [*s. l.*], v. 67, p. 75-88, 2020. Disponível em: https://novaresearch.unl.pt/en/publications/portugal-e-a-revis%C3%A3o-do-conceito-estrat%C3%A9gico-da-nato. Acesso em: 23 out. 2024.

DAEHNHARDT, P. A Resposta da NATO à Nova Ordem Euro-Atlântica Confrontacional. **IDN Brief**, [*s.l.*], p. 1-2, 2022. Disponível em: https://run.unl.pt/handle/10362/167738?mode=full. Acesso em: 23 out. 2024.

DIÁRIO DA REPÚBLICA. **Despacho nº13692/2013**. Orientação Política para a Ciberdefesa. Lisboa: Ministério da Defesa Nacional, 2013.

DIÁRIO DA REPÚBLICA. **Resolução do Conselho de Ministros nº36/2015**. Aprova a Estratégia Nacional de Segurança do Ciberespaço. Lisboa: Presidência do Conselho de Ministros, 2015.

DIÁRIO DA REPÚBLICA. **Resolução do Conselho de Ministros nº92/2019**. Presidência do Conselho de Ministros. Aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023, Lisboa: Ministério da Defesa Nacional, 2019.

DIÁRIO DA REPÚBLICA. **Despacho nº10309/2022**, Parte C, nº163, p.35-36, Gabinete da Ministra. Lisboa: Ministério da Defesa Nacional, 2022a.

DIÁRIO DA REPÚBLICA. **Resolução do Conselho de Ministros nº106/2022**. Presidência do Conselho de Ministros. Aprova a Estratégia Nacional de Ciberdefesa. Lisboa: Ministério da Defesa Nacional, 2022b.

FERNANDES, P. M. **O Conceito Estratégico da NATO (2010): A Perspectiva Portuguesa**. 2013. Tese (Mestrado) - Universidade Nova, Lisboa, 2013.

GARCIA, F. P. O Novo Conceito Estratégico da NATO. **IDN Brief**, [*s. l.*], 2022. Disponível em: https://www.idn.gov.pt/pt/publicacoes/idnbrief/Documents/2022/IDN%20brief%20julho_2022_2_TextoIntegral.pdf. Acesso em: Nov. 2024.

GASPAR, C. O Conceito Estratégico de Madrid. **IDN Brief**, [*s. l.*], 2022. Disponível em: https://www.idn.gov.pt/pt/publicacoes/idnbrief/Documents/2022/IDN%20brief%20julho_2022_2_TextoIntegral.pdf. Acesso em: Nov. 2024.

GERRING, J. Mere Description. **British Journal of Political Science**, Cambridge, v. 42, n. 4, p. 721-746, 2012. DOI: https://doi.org/10.1017/S0007123412000130

MARCELINO, V. Ciberdefesa volta à estaca zero. EMGFA vai agora abrir concurso público internacional. **Diário de Notícias**, Lisboa, 2023. Disponível em: https://www.dn.pt/edicao-do-dia/01-mai-2023/ciberdefesa-volta-a-estaca-zero-emgfa-vai-agora-abrir-concurso-publico-internacional-16262021.html/ Acesso em: Ago. 2024.

NUNES, P. V. **A Edificação da Capacidade de Ciberdefesa Nacional**. 2020. Trabalho (Investigação Individual do CPOG 2019/2020) - Instituto Universitário Militar, Pedrouços, 2020.

NUNES, P. V. **Sociedade em Rede, Ciberespaço e Guerra de Informação**. Contributos para o Enquadramento e Construção de uma Estratégia Nacional da Informação. 2. ed. Lisboa: Instituto da Defesa Nacional, 2016.

NUNES, P. V. Estratégia Nacional de Ciberdefesa. *In*: NUNES, P. (coord.). **IDN Cadernos**. Contributos para uma Estratégia Nacional de Ciberdefesa. Lisboa: Instituto de Defesa Nacional, 2018.

OTAN - Organização do Tratado do Atlântico Norte. Wales Summit Declaration Press Release. **OTAN**, Bruxelas, 2014. Disponível em: https://www.nato.int/cps/en/natohq/official_texts_112964.htm Acesso em: ago, 2024.

OTAN - Organização do Tratado do Atlântico Norte. Strategic Concept. **NATO Summit**, Madrid, 2022. Disponível em: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf. Acesso em: Ago. 2024.

PEREIRA, B. da S. **A Evolução da Relevância do Ciberespaço para a NATO**. 2022. Trabalho (Investigação Individual do CEMC 2021/22) - Instituto Universitário Militar, Pedrouços, 2022.

PEREIRA, R. A. **Desenvolvimento da Capacidade de Ciberdefesa Destacável (NATO CD-DEPLOY)**. 2022. Trabalho (Investigação Individual CPOS-FA 2021/22) - Instituto Universitário Militar, Pedrouços, 2022.

PINHO, P. **O Modelo de Ciberdefesa Nacional: Solução Centralizada ou Distribuída?** 2020. Trabalho (Investigação Individual do CPOS-M) - Instituto Universitário Militar, Pedrouços, 2020.

PIRES, N. de L. **O Novo Conceito de "Multi-Domain Battle" e suas implicações na edificação de capacidades militares no Exército**. 2018. Trabalho (Investigação Individual do CPOG 2017/18) - Instituto Universitário Militar, Pedrouços, 2018.

PORTUGAL. **Conceito Estratégico de Defesa Nacional**. Lisboa: Ministério da Defesa Nacional, 2013a. Disponível em: https://www.defesa.gov.pt/pt/comunicacao/documentos/Lists/PDEFINTER_DocumentoLookupList/Conceito-Estrategico-de-Defesa-Nacional.pdf. Acesso em: Jun. 2023

PORTUGAL. **Resolução do Conselho de Ministros n. 26/2013 de 11 de abril**. Defesa 2020. Lisboa: Ministério da Defesa Nacional, 2013b. Disponível em: https://www.defesa.gov.pt/pt/comunicacao/documentos/Lists/PDEFINTER_DocumentoLookupList/Defesa-2020.pdf. Acesso em: Ago. 2024

PORTUGAL. Ministério da Defesa Nacional. **Despacho n. 13692/2913**. Orientação para a política de Ciberdefesa. Diário da República, n. 208. Lisboa: Ministério da Defesa Nacional, 2013c. Disponível em: https://diariodarepublica.pt/dr/detalhe/despacho/13692-2013-3295679. Acesso em: Ago. 2024.

PORTUGAL. Presidência do Conselho de Ministros. **Resolu**ção do Conselho de Ministros n. **36/2015, de 12 de junho**. Estratégia Nacional de Segurança do Ciberespaço. Diário da República n. 113/2015. Lisboa: Ministério da Defesa Nacional, 2015. Disponível em: https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/36-2015-67468089. Acesso em: Ago. 2024.

PORTUGAL. Presidência do Conselho de Ministros. **Resolução do Conselho de Ministros n. 92/2019 de 5 de junho**. Estratégia Nacional de Segurança do Ciberespaço 2019-2023. Lisboa: Governo de Portugal, 2019.

PORTUGAL. **Despacho n. 2536/2020**. Diretiva Ministerial de Planeamento de Defesa Militar – quadriénio 2019-2022. Diário da República n. 38/2020. Lisboa: Ministério da Defesa Nacional, 2020. Disponível em: https://diariodarepublica.pt/dr/detalhe/despacho/2536-2020-129529718. Acesso em: Ago. 2024.

PORTUGAL. Presidência do Conselho de Ministros. **Resolução do Conselho de Ministros n. 106/2022, de 2 de novembro**. Estratégia Nacional de Ciberdefesa. Diário da República

n. 211/2022. Lisboa: Ministério da Defesa Nacional, 2022a. Disponível em: https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/106-2022-202899924. Acesso em: Ago. 2024.

PORTUGAL. Presidência do Conselho de Ministros. **Decreto-Lei n. 19/2022, de 24 de janeiro**. Lei Orgânica do Estado-Maior-General das Forças Armadas. Diário da República n. 16/2022. Lisboa: Ministério da Defesa Nacional, 2022b. Disponível em: https://diariodarepublica.pt/dr/detalhe/decreto-lei/19-2022-178080766. Acesso em: Ago. 2024.

PORTUGAL. Presidência do Conselho de Ministros. **Decreto-Lei n. 34/2023, de 23 de maio**. Cyber Academia and Innovation Hub. Diário da República n. 99/2023. Lisboa: Ministério da Defesa Nacional, 2023. Disponível em: https://diariodarepublica.pt/dr/detalhe/decreto-lei/34-2023-213345452. Acesso em: Ago. 2024.

PORTUGAL. **O Centro de Ciberdefesa**, s.d. Disponível em: https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa/centro. Acesso em: Ago. 2024.

REIS, B. C. **Pode Portugal ter uma estratégia?** Lisboa: Fundação Francisco Manuel dos Santos, 2019.

REIS, B. C. Uma Nova Estratégia para a NATO vista de Portugal. **IDN Brief**, [*s. l.*], 2022. Disponível em: https://www.idn.gov.pt/pt/publicacoes/idnbrief/Documents/2022/IDN%20brief%20julho_2022_2_TextoIntegral.pdf. Acesso em: Nov. 2024.

RODRIGUES, Alexandre Reis. Considerações sobre o Sistema de Forças Nacional. **Cadernos Navais**, Lisboa, n. 5, p. 1-70, 2003.

RODRIGUES, A. R. **O pensamento de Defesa em Portugal**. Lisboa: Edições Culturais da Marinha, 2020.

SCHWETHER, N. A Guerra do Futuro: comparação das estratégias adotadas pelos Exércitos de Estados Unidos, Espanha e Israel. **Análise Estratégica**, Brasília, DF, v. 21, n. 3, p. 117-149, 2021. Disponível em: http://www.ebrevistas.eb.mil.br/CEEExAE/article/view/8496. Acesso em: 24 out. 2024.

SERRA, M. Até ao fim do ano, Portugal vai quadruplicar os efetivos militares dedicados à ciberdefesa. **TSF Rádio Notícias**, Lisboa, abr. 2019. Disponível em: https://www.tsf.pt/politica/ate-ao-fim-do-ano-portugal-vai-quadruplicar-os-efetivos-militares-dedicados-a-ciberdefesa-10756302.html. Acesso em: Out. 2021.

SERRONHA, M. Portugal e o Novo Conceito Estratégico da NATO. **Relações Internacionais**, [*s. l.*], v. 27, p. 55-66, 2010.

STORTI, D., FERREIRA, M. O Estado como agente inovador nas revoluções nos assuntos militares (RAMs). *In*: ENCONTRO NACIONAL DA ASSOCIAÇÃO BRASILEIRA DE ESTUDOS DE DEFESA, 12., 2022, Niterói. **Anais** [...]. ABED, Niterói, 2022. Disponível em: https://www.enabed2022.abedef.org/resources/anais/19/enabed2022/1658704156_ARQUIVO_c9ff3811d4843661952302187444486f8.pdf. Acesso em: Ago. 2024.